February 19, 2010

Via Electronic Comment Filing System
Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th Street, Suite CY-B402
Washington, DC 20554

Re: American Samoa License, Inc.
CPNI Certification
EB Docket No. 06-36

Dear Ms. Dortch:

On behalf of AST Telecom, LLC dba Blue Sky Communications, pursuant to 47 C.F. R § 64.2009(e), enclosed is its Customer Proprietary Network Information ("CPNI) certification for the 2009 calendar year.

Sincerely,

Adolfo Montenegro

Attachment
cc: Best Copy and Printing, Inc. (via-email)

Annual 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket No. 06-36

Annual 64.2009(e) CPNI Certification for 2009

Date filed: 2/19/2010

Name of company covered by this certification:

AST Telecom, LLC dba Blue Sky Communications

Form 499 Filer ID: 819970

Name of Signatory: Adolfo Montenegro

Title of Signatory: President & CEO

I, Adolfo Montenegro certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. *See* 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, recordkeeping, and supervisory review) set forth in section64.2001 *et seq.* of the Commission's rules.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. 1.17 which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject it to enforcement action.

Signed:_____

Adolfo Montenegro

AST Telecom, LLC
dba BLUE SKY COMMUNICATIONS
CPNI Usage Policy Statement

Pursuant to Section § 64.2009(e) of the Federal Communications Commission's rules, this statement explains how AST Telecom, LLC dba Blue Sky Communication's (the "Company") operating procedures ensure compliance with Part 64, Subpart U, of the FCC's rules.

Company's Usage of CPNI

The Company has chosen to prohibit the use of CPNI for marketing purposes by itself and between affiliates.

The Company has CPNI Procedures that set forth the Company's CPNI policies and outline what CPNI is and when it may or may not be used without customer approval by the Company.

The Company's Procedures provide that the Company may use CPNI to protect its rights and property, customers, and other carriers from fraudulent, abusive or unlawful use of, or subscription to, Company's services.

The Company's Procedures require affirmative written/electronic customer approval for the release of CPNI to third parties.

Company's CPNI Safeguards

The Company has established procedures for the training of its personnel with access to customer CPNI. Employees have been trained as to when they are and are not authorized to use CPNI. The Company's CPNI Procedures describe the disciplinary process related to noncompliance with CPNI obligations. Refresher training courses are often scheduled.

The Company's CPNI Procedures and/or employee manuals contain express disciplinary procedures applicable to employees who violate Company policies, including CPNI policies, which can include termination of employment.

The Company has established a supervisory review process regarding Company compliance with the FCC's CPNI rules. The Company has appointed a corporate officer that has been named as the CPNI Compliance Officer and is held responsible for annually certifying that the Company is in compliance with the FCC's CPNI rules and submitting such certification and accompanying statement of how the company complies with the FCC's CPNI rules to the FCC by March 1st.

The Company takes reasonable measure to discover and protect against attempts to gain unauthorized access to CPNI. Company authenticates a customer prior to disclosing CPNI based on customer initiated telephone contact or an in-store visit.

The Company only discloses call detail information over the telephone, base on customer-initiated telephone contact, if the customer first provides a password that is not prompted by the carrier asking for readily available biographical information or account information. If a customer does not provide a password, Company only discloses call detail information by sending it to an address of record or by calling the customer at the telephone of record. If the customer is able to provide call detail information during a customer-initiated call without Company's assistance, then Company is permitted to discuss the call detail information provided by the customer.

The Company has established a system of passwords and password protection. For a new customer (a customer that establishes service after the effective date of the new CPNI rules), Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, the customer must visit one of the two retail stores at which time the representative must establish that the person at the counter is indeed the registered person whose name is on the account by valid photograph identifications such as a Passport, Government ID, Driver's license and/or Immigration ID.

For accounts that are password protected, Company cannot obtain the password by asking for readily available biographical information or account information to prompt the customer for his password. If a password is forgotten or lost, Company uses a backup customer authentication method that is not based on readily available biographical information or account information.

If a customer does not want to establish a password, the customer may still access call detail based on a customer-initiated telephone call, by asking Company to send the call detail information to an address of record or by the carrier calling the telephone number of record.

If a customer is able to provide to the Company, during a customer-initiated telephone call, all of the call detail information necessary to address a customer service issue (i.e., the telephone number called, when it was called, and if applicable, the amount charged for the call) then Company proceeds with its routine customer carrier procedures. Under these circumstances, Company may not disclose to the customer any call detail information about the customer account other than the call detail information that the customer provides without the customer first providing a password.

Company may provide customers with access to CPNI at a carrier's retail location if the customer presents a valid photo ID and the valid photo ID matches the name on the account. Company, at this time, does not provide on-line access.

Company notifies a customer immediately when a password, customer response to a back-up means of authentication for lost or forgotten passwords, or address of record in created or changed by mail to the address of record.

In the event of a CPNI breach, Company delays customer notification of breaches until

law enforcement has been notified of a CPNI breach. Company will notify law enforcement of a breach of its customers' CPNI within seven business days after making a reasonable determination of a breach by sending electronic notification through a central reporting facility to the United States Secret Service (USSS) and the FBI. If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, that agency may direct Company not to disclose the breach for an initial 30-day period. The law enforcement agency must provide in writing to the carrier its initial direction and any subsequent direction.

Company, however, may immediately notify a customer or disclose the breach publicly after consultation with the relevant investigative agency, if Company believes there is an extraordinarily urgent need to notify a customer of class of customers to avoid immediate and irreparable harm.

Company maintains a record of any discovered breaches and notification to the USSS and the FBI regarding those breaches, as well as the USSS and the FBI response to the notification for a period of at least two years.

Actions Taken Against Data Brokers and Customer Complaints

Company has taken no actions against data brokers in the past year. Company has received no customer complaints in the past year concerning the unauthorized release of CPNI.